数理解析研究所講究録
81巻 1970年 338-367

Fail-Safe論理系の構成について

浦野義頼

（早稲田大学大学院）

第1章 序言

システムの大形化，複雑化に伴い，システム内に障害が発生しても常に安全側に落着く，いわゆる"Fail-Safe"システムの重要性が高まりつつある。

本稿は，このような"Fail-Safe"システムの構成に関する筆者らの最近の研究結果をまとめたものである。

本章では，"Fail-Safe"の基本的概念を明らかにし，各種のFail-Safe論理系を定義する。

次に，このようなFail-Safe論理系研究の発端となった，"0"〔"1"〕形Fail-Safe論理系の構成を論ずる。（第2章）

第3章においては，"0"（"1"）形Fail-Safe論理系が有する問題点の解決策として筆者らが提唱する"Ⅱ"形Fail-Safe論理系について，（i）多値論理（システム）に占める位置（ii）多値論理からみた諸性質等の検討を行う。

最後に新しい2重系，交番論理系について考察する。（第4章）

1．1．"Fail-Safe"の概念

一般に，システムの安全性は人間的な要素を無視し得ないのであるが，ここでは当面の問題として純粋に工学的な立場から論ずることにする。このとき，"Fail-Safe"という概念はいかに定義されるであろうか。

"Fail"，"Safe"のいずれにも概念の広がりが存在するから，統一的解釈を与えることは難しいが，現実に"Fail-Safe"と称されているシステムを参考にして，広義"Fail-Safe"を次のような概念を包含するものとして定義するのが妥当と思われる。

(i) 狭義信頼性 (Reliability)

部分システムの"Fail"が全システムの"Fail"(特に論理的，機能的障害，故障)とならない。(能力の低下はない。)

(ii) 狭義 Fail-Safe

ある部分システムの"Fail"は全システムの機能的障害，故障状態を招くが，それらは予め"安全側の許容障害，故障状態"と指定されたものに限られる。

(iii) Fail-Soft (Graceful Degradation)

部分システムの"Fail"によって全システムの能力(能率，効率)の低下となるが，システム全体の機能的障害，故障とならない。(機能的障害，故障が局所的。)

(iv) Fool-Proof (Fail-Proof)

特に人間－機械システムにおいて，人間工学的な観点から，人間がおかす機械の取扱い誤りをなくしたり，誤って取扱っても危険でないようにする。

このように，広義"Fail-Safe"なる概念はさらに幾つかに細分されるが，それらは互いに重なり合う場合も少なくない。本稿では狭義"Fail-Safe"について考察する。

1．2 Fail-Safe論理系

前節で述べたFail-Safeの概念を論理システム（論理系）に適用するとき，狭義Fail-Safe論理系が次のように定義される。

Fail-Safe論理系は，"その部分論理系に障害が生起するとき，予め指定された論理動作：安全側の故障状態に入る（例えば，許容出力すなわち，誤りとならない出力あるいは予め定められた安全側許容誤り出力を発生する）論理系"である。

このとき，予め指定される論理動作（安全側故障状態，安全側の許容誤り出力）の設定の仕方により各種のFail-Safe論理系が定義されるのである。以下の各章参照。

第2章 "0"〔"1"〕形 Fail-Safe 論理系

2．1 "0"〔"1"〕形 Fail-Safe 論理系

論理系の Fail-Safe 性に関して対象とする故障を次のように限定しておく。論理系に生ずる障害（故障）は，その部分論理系が，

（ⅰ）機能障害（誤り論理動作）となるもの

（ⅱ）機能障害（誤り論理動作）とならないもの

に類別されるが，"論理"の立場から前者についてのみ考察するものとする。更に，論理システムの構造を考慮し，また，その議論を簡単にする為，以後，特に基本論理（回路）の stuck（固定）故障のみ取扱うものとする。

従って，その部分論理系に"0"固定故障および/または"1"固定故障の生起が予想される2値（"0"，"1"）論理系では"0"〔"1"〕形 Fail-Safe 論理系が以下のように定義される。

〔定義 2．1〕 安全側の許容誤り出力は 1→0 形（"0"形）〔0→1 形（"1"形）〕であるとする。その構成部品に"0"固定および/または"1"固定故障が発生するとき，論理系が許容出力即ち，論理的に正しい出力あるいは"0"〔"1"〕形誤り（故障）出力を有するならば この論理系は"0"〔"1"〕形 Fail-Safe（論理系）であるという。

換言すれば，与えられた論理関数 $f(X)$ を実現する論理系 S_f が"0"〔"1"〕形 Fail-Safe であるというのは，

S_f に可能な全ての故障 ε_i について

条件 I. $0 \subseteq F_{\varepsilon_i}(X) \subseteq f(X)$

〔条件 II. $1 \supseteq F_{\varepsilon_i}(X) \supseteq f(X)$ 〕

となることである。但し，故障論理関数 $F_{\varepsilon_i}(X)$ は故障 ε_i が生起する際の論理系の出力論理関数である。

このような論理系では次のような結果が得られている。

〔定理 2.1〕 論理関数 $f(X)$ を実行する非冗長論理系は同一点に"0"固定故障と"1"固定故障の両方が生起可能であるとき Fail-Safe となり得ない。

〔定理 2.2〕 所与の論理関数，

$$f(X)=f(g_1(X),\ g_2(X),\ \cdots,\ g_i(X),\ \cdots)$$

を実行する論理系 S_f が，その部分論理関数 $g_i(X)$ の"α"固定故障（$\alpha=0$ or 1）と等価な故障 ε_α をもつとき，この論理系が故障 ε_α に対して"Fail-Safe"である為には，$f(X)$ は $g_i(X)$ に関して unate でなければならない。

"0"〔"1"〕形 Fail-Safe 論理系は，その構成を論ずるとき次のように分類するのが実用的である。

〔定義 2．2〕 "0"〔"1"〕形 Fail-Safe 論理系において，特定な入力誤り（故障）についても条件 I〔条件 II〕が成立するとき，その論理系は "Strongly" "0"〔"1"〕形 Fail-Safe であるといい，それらの入力を "許容誤り入力" あるいは "Fail-Safe 入力" と呼ぶ。この "許容誤り入力"（"Fail-Safe" 入力"）をもたぬものは "Weakly" "0"〔"1"〕形 Fail-Safe 論理系と称される。

〔定理 2．3〕 基本論理回路が (i) Strongly (ii) Weakly "0"〔"1"〕形 Fail-Safe である為の必要十分条件は，
その出力論理関数が (i) unate であり，(ii) unate でなくかつ，可能な出力故障が "0"〔"1"〕固定故障である。

2．2．交番則の適用による "0"〔"1"〕形 Fail-Safe 論理系の構成

〔定義 2．3〕 "許容誤り出力割当に関する交番則"

"許容誤り出力割当に関する交番則"（"交番則"）は，与えられた論理関数 $f(X)$ を遂行する Strongly（Weakly）"α" 形 Fail-Safe 論理系実現の為に，構成要素である各基本論理回路に許容される誤り出力の形（type）を割当てる規則で，"否定論理を含む基本論理回路" に関して α，$\bar{\alpha}$ なる許容誤り出力状態を

交番的に割当てるものである。ここで"否定論理を含む基本論理回路"は，その出力論理関数 $f(X_i)$ が入力変数 X_i に関して負であるものを意味する。$\alpha = 0$ or 1

［定理 2. 4］　与えられた論理関数 $f(X)$ を実行する論理系が (i) Strongly，(ii) Weakly "α" 形 Fail-Safe であるための必要十分条件は

(i) 交番則により矛盾なく割当てられた許容誤り出力 "α_j" を有する Strongly "α_j" 形 Fail-Safe 基本論理回路：$f_j(X)$ から構成される，

(ii) error-free 入力という仮定のもとで交番則を適用するとき矛盾なく割当てられた許容誤り出力 "α_k"（"α_l"）を有する Weakly "α_k" 形 Fail-Safe 基本論理回路 $f_k(X)$（および Strongly "α_l" 形 Fail-Safe 基本論理回路 $f_l(X)$）から構成される

ことである。α, α_j, α_k, $\alpha_l = 0$ or 1

尚，一般に Strongly Fail-Safe 論理系の場合，同一入力変数について複数個の基本回路から2種の許容誤り入力が別々に要請されるとき，系は Pseudo-Strongly Fail-Safe であるということがある。（non-unate 論理関数は Pseudo-Strongly Fail-Safe あるいは Weakly Fail-Safe 論理系として実現される。）

第3章 "亜"形 Fail-Safe 論理系

3.1 "亜"形Fail-Safe論理系

前章で述べた"0"〔"1"〕形Fail-Safe論理系は

(i) "0"〔"1"〕形出力誤りは許容される,

(ii) 部分論理系に"0"固定かつ/または"1"固定故障の生起可能,

という前提に立つものであるから次の問題を含んでいる。

問題1. "0"〔"1"〕形Fail-Safe論理系においてはその出力,"0"〔"1"〕の正誤が決定不能。そのため,故障検査が困難。

問題2. 任意の論理関数を"0"〔"1"〕形Fail-Safe論理系として実現しようとするとき,実存する物理系で理想的なものとして得ることが難しい場合もある。

問題3. 論理系に生ずる障害で"0"固定かつ/または"1"固定故障を仮定しえないことがある。

問題4. システムに課せられた目的によっては"論理動作の判定が未定または中止となり,誤り状態であることを明示可能"は許容されるが,誤って"0","1"の出力を発生することは許されない場合が考えられる。

以上の点を考慮して筆者らは,障害発生時の出力誤りが"0","1"に等しくない"亜"形故障論理系,"亜"形誤り出力を許容誤り出力とする"亜"形Fail-Safe論理系を提唱した。

〔定義3．1〕　正常動作時の論理系の"0"状態（出力，真理値）および"1"状態（出力，真理値）とdisjointである状態（出力，真理値）；"Φ"に固定するものを"Φ"形故障（"Φ"固定故障）という。正常動作状態（出力，真理値）集合をΨ＝{"0"，"1"}で表わすとき，

$$\Psi \cap \Phi = \emptyset \text{（空）}$$

である。

ある2値（"0"，"1"）論理系 $f(X) = f(X_1, X_2, \cdots, X_m)$ の構成要素に生起可能な故障（誤り）が"Φ"形故障のみであるとき，系は"Φ"形故障（基本）論理系であるといわれ，以下のように定式化される。

I．正常動作状態

$$f[{}^{(k)}X_{i_1}, {}^{(k)}X_{i_2}, \cdots, {}^{(k)}X_{i_r}, {}^{(l)}X_{j_1}, {}^{(l)}X_{j_2}, \cdots, {}^{(l)}X_{j_s}]$$

（$f[{}^{(k)}X(i,r), {}^{(l)}X(j,s)]$ と略記する）

$$\triangleq \{\Psi\} = \{\text{"0"}, \text{"1"}\}$$

但し，$X(i,r) \cup X(j,s) = X$，$X(i,r) \cap X(j,s) = \emptyset$（空）

(k)は r－組（$X_{i_1}, X_{i_2}, \cdots, X_{i_r}$），（$X_{i_k} = 0$ or 1）のk番目の組合わせ，(l)は s－組（$X_{j_1}, X_{j_2}, \cdots, X_{j_s}$），（$X_{j_k} = 0$ or 1）のl番目の組合わせを表示する。

II．故障動作状態

（i）"Φ"形入力故障の場合　変数X_lが"Φ"状態に固

定する故障を${}^{[\text{亜}]}X_i$とすれば，一般に"亜"形入力故障は

$$f[{}^{(k)}X_{i_1},\ {}^{(k)}X_{i_2},\ \cdots,\ {}^{(k)}X_{i_r},\ {}^{[\text{亜}]}X_{j_1},\ {}^{[\text{亜}]}X_{j_2},\ \cdots,\ {}^{[\text{亜}]}X_{j_s}]$$

（$f[{}^{(k)}X_{(i,r)},\ {}^{[\text{亜}]}X_{(j,s)}]$ と略記）

と表わされる。

(a) "亜"形入力故障に対応する，ある l, l' について，

$$f[{}^{(k)}X_{(i,r)},\ {}^{(l)}X_{(j,s)}] \neq f[{}^{(k)}X_{(i,r)},\ {}^{(l')}X_{(j,s)}]$$

であるとき，$f[{}^{(k)}X_{(i,r)},\ {}^{[\text{亜}]}X_{(j,s)}] \mathrel{\hat{=}} \{\text{亜}\}$

(b) "亜"形入力故障に対応する，全ての l, l' について

$$f[{}^{(k)}X_{(i,r)},\ {}^{(l)}X_{(j,s)}] = f[{}^{(k)}X_{(i,r)},\ {}^{(l')}X_{(j,s)}]$$

であるとき，$f[{}^{(k)}X_{(i,r)},\ {}^{[\text{亜}]}X_{(j,s)}] \mathrel{\hat{=}} \{\text{亚}\}$ or $\{\text{亜}\}$

（亚/亜 で表示）

(ii) "亜"形出力故障の場合　論理系自体の出力故障は入力とは無関係に"亜"形誤り出力となる。

$${}^{[\text{亜}]}f[{}^{(k)}X_{(i,r)},\ {}^{(l)}X_{(j,s)}] = {}^{[\text{亜}]}f[{}^{(k)}X_{(i,r)},\ {}^{[\text{亜}]}X_{(j,s)}]$$

$\mathrel{\hat{=}} \{\text{亜}\}$

この定義において，条件 II.(i).(b) における任意性が論理系の情報曖昧さの程度を規定する。例えば，ここで

$$f[{}^{(k)}X_{(i,r)},\ {}^{[\text{亜}]}X_{(j,s)}] \mathrel{\hat{=}} \text{亚}\,[\text{亜}]$$

とすれば，系の情報曖昧さが最小〔最大〕となる。（このとき，"亜m"("亜M")形故障論理系という。）

従って，一般の“Φ”形故障論理系は，それらの論理系を両極限として定義されるのである。

〔定義 3. 2〕 安全側にある許容誤り出力が“Φ”形（“0”→“Φ”形 および/または “1”→“Φ”形）であるとする。このとき，ある論理系に生起する，いかなる障害に対しても安全側の許容出力をとるならば，即ち，可能な誤り出力が“Φ”形誤り出力に限られるならば，系は“Φ”形 Fail-Safe 論理系であるという。
（尚，最小〔最大〕情報曖昧さを有する“Φ”形 Fail-Safe 論理系は“Φ_m”〔“Φ_M”〕形 Fail-Safe であるという。）
このとき，『“Φ”形故障（基本）論理系を構成要素とする論理系は，“Φ”形 Fail-Safe 論理系である。』但し，論理系への入力は論理的に誤りがないか，あるいは“Φ”形誤り（故障）に限定されるものとする。

3. 2 3レベル（0，φ，1）“Φ”形 Fail-Safe 論理系

前項で“Φ”形故障論理系の構造と“Φ”形 Fail-Safe 論理系の存在可能性について述べてきたが，以下の節では実際の物理系との対応を考慮しながら具体的な検討を行う。特に，3レベル：0，φ，1をもつ（Single Rail）論理系と Double

Fail論理系について考察する。（ここで，ϕは故障状態（出力，真理値）を表わすものとする。）

A. "Ⅱ"形故障（"Ⅱ"形Fail-Safe）基本論理回路

3レベル：0，ϕおよび1をもつ，2値（"0"，"1"）論理系は以下の"Ⅱ"形故障（Fail-Safe）基本論理回路により構成される。但し，正常状態（真理値）：Ⅰ ≜ {0，1}

故障状態（真理値）：Ⅱ ≜ {ϕ}

ここでは2変数論理関数の場合について述べるが多変数論理関数回路への拡張も同様になされる。

1）"Ⅱ"（"ϕ"）形故障（Fail-Safe）論理和回路：${}^{\phi}\vee$

2変数"ϕ"形故障（Fail-Safe）論理和回路：${}^{\phi}\vee$ は，図.3.1.(a)に示す真理値表により規定されるものである。表中の$1/\phi$は対応の出力が"1"または"ϕ"であることを意味するもので，（但し，$1/\phi$は，一般には，それが占める座標の関数である），そのいずれをとるかが論理系の情報曖昧さを規定する。すぐわかるように，表中の全ての$1/\phi$について

$1/\phi$ ≜ 1〔ϕ〕とするとき，最小〔最大〕情報曖昧さの

論理系 ${}^{\phi_m}\vee$ 〔${}^{\phi_M}\vee$〕

となる。

"ϕ"形故障（誤り）入力に対応する，論理回路：${}^{\phi}\vee$ の出力の中で"ϕ"は誤りであるが，"1"は論理的に正しい出

力である。

以上，基本論理回路の故障状態として入力の"亜("φ")形故障のみ扱っているが，これは次の仮定に立つからである。

仮定 1. 部分論理系の出力故障は"亜"形故障に限られる。

仮定 2. ある部分論理系の"亜"形出力故障は次の部分論理系への入力"亜"形故障(誤り)と等価である。

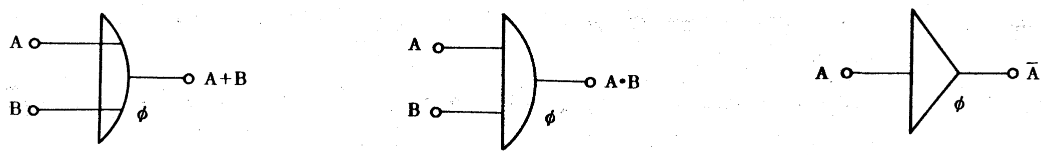
これらの仮定は後述の論理回路についても成立するものである。

2) "亜"("φ")形故障(Fail-Safe)論理積回路：$^{\phi}\wedge$

$^{\phi}\wedge$ は $^{\phi}\vee$ と双対的な性質がある。図 3. 1. (b) 参照。

3) "亜"("φ")形故障(Fail-Safe)論理否定回路：$^{\phi}N$

図 3. 1. (c) の真理値表により規定される。



A \ B	0	φ	1
0	0	φ	1
φ	φ	φ	1/φ
1	1	1/φ	1

(a) $^{\phi}\vee$

A \ B	0	φ	1
0	0	0/φ	0
φ	0/φ	φ	φ
1	0	φ	1

(b) $^{\phi}\wedge$

A	Ā
0	1
φ	φ
1	0

(c) $^{\phi}N$

図 3. 1. "亜"("φ")形 Fail-Safe 基本論理回路

B. 基本論理回路：$^{\phi}V$，$^{\phi}\wedge$，$^{\phi}N$ による３レベル“亜”形 Fail-Safe 論理系の構成

『任意に与えられた論理関数 f（X）は，A. で定義した基本論理回路：$^{\phi}V$，$^{\phi}\wedge$，$^{\phi}N$ により“亜”形 Fail-Safe論理系として実現される。』

３．３．多値論理からみた“亜”形 Fail-Safe論理系の構造

A. 多値論理に占める“亜”形 Fail-Safe 論理系の位置

従来の多値論理研究においては主として完全性について論じられている。ところで“亜”形 Fail-Safe論理系も一種の多値論理系であるが，

（i）M値（$M = |\{亜\}| + |\{亜\}|$）論理を２値（$2 = |\{亜\}|$）論理に縮退して用い，残りの真理値には実際に意味のある論理値として使われる情報以外の情報，即ち“亜”形故障発生という情報が与えられる，

（ii）M値論理として完全でないが２値論理として完全である

ことを活用している点に特徴がある。

このように，一般に完全でないM値論理（系）を完全なるN値論理（系）に縮退させて用いることにより付加的な情報をもたせたり，逆にN値論理（系）をM値論理（系）に拡

張することによってその構造を見やすくすることが期待されるから，このような多値論理の見方は重要と思われる。

B.　Kleeneの3値論理と"ϕ_m"形Fail-Safe論理系

S. C. Kleeneが提唱した3値論理システムは，次のone-to-one対応を考えるとき，"Φ"形（"ϕ_m"形）Fail-Safe論理系の構造を調べるのに適していることがわかる。

	"ϕ_m"形Fail-Safe論理系	Kleene論理
真理値	$\Psi = \{0, 1\}$	Ⅰ，Ⅲ
	$\Phi = \{\phi\}$	Ⅱ
順序付け	$0 \subset \phi \subset 1$	Ⅰ ⊂ Ⅱ ⊂ Ⅲ
基本演算	${}^{\phi_m}\vee(X, Y)$	加法＋：$X + Y = \mathrm{Max}(X, Y)$
	${}^{\phi_m}\wedge(X, Y)$	乗法・：$X \cdot Y = \mathrm{Min}(X, Y)$
	${}^{\phi_m}N(X)$	否定$^{-}$：$\overline{X}$ = Ⅳ − X

定義域 L_1 = {Ⅰ，Ⅱ，Ⅲ} で定義される3値Kleene論理系の基本演算（論理）：＋，・，$^{-}$を定数または変数（X_1, X_2, ---, X_n）に繰返し適用することにより得られる論理関数，3値Kleene論理関数を$f_K(X)$で表わすことがある。この3値Kleene論理関数$f_K(X)$は定義域をL_2 = {Ⅰ，Ⅲ} に制限すれば，2値（Ⅰ，Ⅲ）Boole論理関数$f_B(X)$を生成する。換言すれば，上述の対応を考えるとき，"ϕ_m"形Fail-Safe

基本論理回路からなる論理系の論理動作は 入力"Ⅱ"("φ")形故障(誤り)を含めて3値Kleene論理により記述されるのである。

Kleene論理の基本的性質

冪等律, 交換律, 結合律, 吸収律, 分配律, 二重否定および de Morganの法則; $\overline{X+Y} = \overline{X}\cdot\overline{Y}$

$$\overline{X\cdot Y} = \overline{X}+\overline{Y}$$

の成立するのは2値のBoole代数と同様である。但し, 次の性質には注意したい。

(i) $X\cdot Y + X\cdot\overline{Y} \subseteq X$

$$(X+Y)\cdot(X+\overline{Y}) \supseteq X$$

(ii) $g_K{}^1 = X_i^{\alpha}\cdot X_j^{\beta}\cdot X_k^{\gamma}$, $g_K{}^2 = X_i^{\overline{\alpha}}\cdot X_j^{\beta}\cdot X_k^{\gamma}$

$g_K{}^3 = X_i^{\alpha}\cdot X_j^{\beta}\cdot X_k^{\overline{\gamma}}$, $g_K{}^4 = X_i^{\alpha}\cdot X_j^{\overline{\beta}}\cdot X_k^{\overline{\gamma}}$

のとき $\sum_{i=1}^{4} g_K^i \subseteq X_j^{\beta}\cdot X_k^{\gamma} + X_i^{\alpha}\cdot X_k^{\overline{\gamma}}$

$$\subseteq X_j^{\beta}\cdot X_k^{\gamma} + X_i^{\alpha}\cdot X_k^{\overline{\gamma}} + X_i^{\alpha}\cdot X_j^{\beta}$$

$$(\triangleq f_K^*(X_i,\ X_j,\ X_k))$$

但し, $\alpha,\ \beta,\ \gamma = 0$ or 1, $X^0\,(X^1) = \overline{X}\ (X)$

$X_i,\ X_j,\ X_k = \{\mathrm{I},\ \mathrm{III}\}$ ならば, $\sum_{i=1}^{4} g_K^i = f_K^*(X_i, X_j, X_k)$

$\sum_{i=1}^{4} g_K^i = \mathrm{I}$ ならば, $f_K^*(X_i, X_j, X_k) = \mathrm{I}$

積和形式で述べた性質（ii）に双対の結果が和積形式について得られる。

このような3値Kleene論理の性質を活かすことにより，"Φ"（"φ"）形Fail-Safe論理系の（ある意味で）最適な構成法が得られる。（C. 参照）

C. "ϕ_m" 形 Fail-Safe 論理系の最適構成法

与えられた論理関数 $f(X)$ を前述の "ϕ_m" 形 Fail-safe 基本論理回路：${}^{\phi_m}\vee$，${}^{\phi_m}\wedge$，${}^{\phi_m}N$ により実現する際 論理系の入力 "ϕ" 形故障（誤り）に対して最小情報曖昧さをもつ構成がある。（この手法は M.Yoeli, E.B. Eichelberger らの hazard free network 構成法と全く同様に考えられるものであるから 詳細は省略する。）

"全ての主項の和で表わされた2値論理関数 $f_B^*(X)$ の各2値論理：論理和（OR），論理積（AND），論理否定（NOT）をそれぞれ，${}^{\phi_m}\vee$，${}^{\phi_m}\wedge$，${}^{\phi_m}N$ で実現する論理系は "Φ_m"（"ϕ_m"）形 Fail-Safe である。"

一般に，"ϕ_m" 形 Fail-safe 基本論理回路：${}^{\phi_m}\vee$，${}^{\phi_m}\wedge$，${}^{\phi_m}N$ よりなる論理系は，"ϕ_m" 形 Fail-safe 性に関して閉じていない。従って，上に提案された構成法はその点からも興

味深い。

D. "ϕ_m" 形 Fail-Safe 論理系の閾値論理実現

"ϕ_m" 形 Fail-Safe 論理系の論理動作を記述する3値（0，ϕ，1）論理関数の導出を行い，その閾値実現を試みる。このような一般3値論理関数において単一閾値素子で実現される類は限られており，多閾値素子構成の論議も容易でない。

そこで，任意の論理関数を反転入力の導入により対称化することができる事実を利用すること等により，対称論理関数として実現する方法が考えられる。

3．4． "Φ" 形 Fail-Safe Double Rail 論理系

前述のように，3レベル（0，ϕ，1）"Φ"（"ϕ"）形 Fail-Safe 論理系の構成は，基本論理回路：ϕ_V，ϕ_Λ，ϕ_N の存在という仮定に立つのであるが，ϕ_N の物理的実現が不能（困難）な場合も予想される。

筆者らが提唱した "Double Rail" 論理系の概念は，この難点を避けることができるだけでなく，故障検査などにおいて多くの利点を有していることも示される。

Double Rail 論理系は J. Von Neumann の "Double Line Trick" を応用したもので，2つの信号線（線路）よりなる。この論

理系は、論理変数 X_i が（X_i，x_i）のように対の信号（符号）：大文字 X_i と小文字 x_i の組合わせで表示され、

真理値 "0" と 符号（0，1）

真理値 "1" と 符号（1，0）

なる対応のもとで所定の論理（関数）を実行するものである。残りの 2-tuple は故障（誤り）を表わす。

3レベル（0，ϕ，1）を有する Double Rail 2値｛"0"（0，1），"1"（1，0）｝論理系として図．3．2に示す3基本論理回路；

"ϕ" 形 Fail-Safe Double Rail 論理和回路：${}^{\phi}V_d$

"ϕ" 形 Fail-safe Double Rail 論理積回路：${}^{\phi}\wedge_d$

"ϕ" 形 Fail-safe Double Rail 論理否定回路：${}^{\phi}N_d$

からなるものを考える。

これらの基本論理回路は、

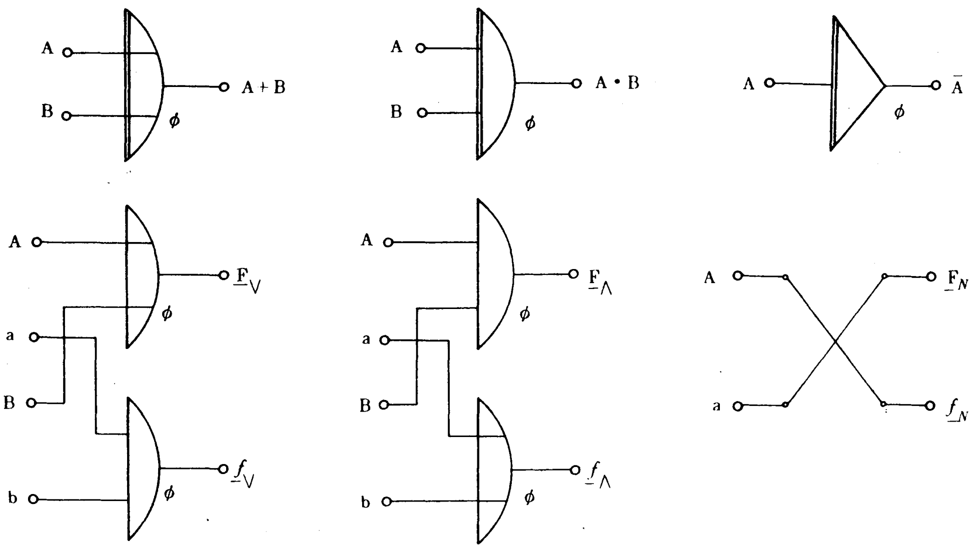
$\Sigma \triangleq$ ｛"0"（0，1），"1"（1，0）｝

$\Phi \triangleq$ ｛（0，ϕ），（ϕ，0），（ϕ ϕ）（ϕ，1），（1，ϕ）｝

とするとき、"Φ" 形故障論理系 "Φ" 形 Fail-Safe 論理系であることがわかる。

表．3．1．${}^{\phi}V_d$，${}^{\phi}N_d$ の真理値表

表 3．2．${}^{\phi}V_d$，${}^{\phi}N_d$ の誤り出力表



(a) $^{\phi}$Vd (b) $^{\phi}\wedge$d (c) $^{\phi}$Nd

図 3. 2 $^{\phi}$Vd, $^{\phi}\wedge$d, $^{\phi}$Nd の構成

表 3. 1 $^{\phi}$Vd, $^{\phi}$Nd の真理値表

(a) $^{\phi}$Vd

A	B \ Aa \ Bb			0					1	
		0 0	0 φ	0 1	φ 0	φ φ	φ 1	1 0	1 φ	1 1
	0 0	0 0	0 ${}^{0}/_{\phi}$	0 0	φ 0	φ ${}^{0}/_{\phi}$	φ 0	1 0	1 ${}^{0}/_{\phi}$	1 0
	0 φ	0 ${}^{0}/_{\phi}$	0 φ	0 φ	φ ${}^{0}/_{\phi}$	φ φ	φ φ	1 ${}^{0}/_{\phi}$	1 φ	1 φ
0	0 1	0 0	0 φ	0 1	φ 0	φ 0	φ 1	1 0	1 φ	1 1
	φ 0	φ 0	φ ${}^{0}/_{\phi}$	φ 0	φ 0	φ ${}^{0}/_{\phi}$	φ 0	${}^{1}/_{\phi}$ 0	${}^{1}/_{\phi}$ ${}^{0}/_{\phi}$	${}^{1}/_{\phi}$ 0
	φ 0	φ ${}^{0}/_{\phi}$	φ φ	φ φ	φ ${}^{0}/_{\phi}$	φ φ	φ φ	${}^{1}/_{\phi}$ ${}^{0}/_{\phi}$	${}^{1}/_{\phi}$ φ	${}^{1}/_{\phi}$ φ
	φ 1	φ 0	φ φ	φ 1	φ 0	φ φ	φ 1	${}^{1}/_{\phi}$ 0	${}^{1}/_{\phi}$ φ	${}^{1}/_{\phi}$ 1
1	1 0	1 0	1 ${}^{0}/_{\phi}$	1 0	${}^{1}/_{\phi}$ 0	${}^{1}/_{\phi}$ ${}^{0}/_{\phi}$	${}^{1}/_{\phi}$ 0	1 0	1 ${}^{0}/_{\phi}$	1 0
	1 φ	1 ${}^{0}/_{\phi}$	1 φ	1 φ	${}^{1}/_{\phi}$ ${}^{0}/_{\phi}$	${}^{1}/_{\phi}$ φ	${}^{1}/_{\phi}$ φ	1 ${}^{0}/_{\phi}$	1 φ	1 φ
	1 1	1 0	1 φ	1 1	${}^{1}/_{\phi}$ 0	${}^{1}/_{\phi}$ φ	${}^{1}/_{\phi}$ 1	1 0	1 φ	1 1

(b) $^{\phi}$Nd

A	Aa	$\overline{\text{Aa}}$
	0 0	0 0
	0 φ	φ 0
0	0 1	1 0
	φ 0	0 φ
	φ φ	φ φ
	φ 1	1 φ
1	1 0	0 1
	1 φ	φ 1
	1 1	1 1

表 3.2 誤り出力表

(a) $^{\phi}\vee_{d}$

"Φ" failure input	Output
$(0\phi)^{\Delta}$ $(\phi 0)^{\Delta}$ $(\phi\phi)$ $(\phi 1)^{\Delta}$ $(1\phi)^{\Delta}$	$(0\phi)^{\Delta}$ $(\phi 0)^{\Delta}$ $(\phi\phi)$ $(\phi 1)^{\Delta}$ $(1\phi)^{\Delta}$ $(10)^{◎}$
$(00)^{\bigstar}$ $(11)^{\bigstar}$	

(b) $^{\phi}N_{d}$

"Φ" failure input	Output
$(0\phi)^{\Delta}$ $(\phi 0)^{\Delta}$ $(\phi\phi)$ $(\phi 1)^{\Delta}$ $(1\phi)^{\Delta}$	$(0\phi)^{\Delta}$ $(\phi 0)^{\Delta}$ $(\phi\phi)$ $(\phi 1)^{\Delta}$ $(1\phi)^{\Delta}$
$(00)^{\bigstar}$ $(11)^{\bigstar}$	

3．5．"Φ_0"〔"Φ_1"〕形 Fail-Safe Double Rail 論理系

基本論理回路：$^{\phi}\vee$，$^{\phi}\wedge$ からなる "Φ" 形 Fail-Safe Double Rail 論理系の概念は第２章で述べた "0"〔"1"〕形 Fail-safe 基本論理回路：$^{0}\vee$，$^{0}\wedge$〔$^{1}\vee$，$^{1}\wedge$〕により構成される Double Rail 論理系に拡張される。

論理回路：$^{\phi}\vee$ および $^{\phi}\wedge$ をそれぞれ論理回路：$^{0}\vee$ および $^{0}\wedge$（$^{1}\vee$ および $^{1}\wedge$）で置換えることにより実現される Double Rail 論理和回路，論理積回路を $^{\phi_0}\vee_d$，$^{\phi_0}\wedge_d$（$^{\phi_1}\vee_d$，$^{\phi_1}\wedge_d$）で表わす。論理回路：$^{\phi_0}N_d$〔$^{\phi_1}N_d$〕は $^{\phi}N_d$ と全く同じもの，即ち，２つの信号線を単純に交叉させたものとする。

ここで，

$$\Phi = \{\text{"0"}(0,1),\ \text{"1"}(1,0)\}$$

$$\Phi_0 = \{(0,0)\}$$

$$\left\lceil\ \Phi = \{\text{"0"}(0,1),\ \text{"1"}(1,0)\}\right.$$

$$\Phi_1 = \{(1,1)\}$$

であるとすれば，このような論理回路：${}^{\phi_0}\vee_d$，${}^{\phi_0}\wedge_d$，${}^{\phi_0}N_d$〔${}^{\phi_1}\vee_d$，${}^{\phi_1}\wedge_d$，${}^{\phi_1}N_d$〕は"Φ"形故障，Fail-Safe 論理系である。

従って，これらの基本論理回路を用いれば，任意の論理関数 $f(X)$ は"Φ_0"〔"Φ_1"〕形 Fail-Safe Double Rail 論理系として実現される。

第4章　交番論理系

最後に，Double Rail 論理系（第3章）において空間に置いた冗長性を時間領域に拡張した“交番論理系”について簡単に述べる。

論理系の高信頼度化のため冗長性を導入する多重化（2重化）法は古くから知られている技法であるが，実用的効果として

（i）部分論理系の故障はシステム・ダウンとならず，所定の使命が遂行される

（ii）故障検査（検出，診断）容易な機構（構造）を与える

ことが考えられる。従来，主として前者の観点から論議がなされており，後者は2次的なものとみなされてきた。また，論理系の処理速度より安全性が重要視され，第2の特質を活用するため2重化を積極的に採用することが望まれても，それに伴う費用の増大などから用いられないことも少なくない。

従って，ハードウェアの増加をできる限り小さくし，（少なくとも単純な2重化系より低 cost で），2重化論理系の特徴を活かしたいという要請が生じてくる。この要請に応えるものとして次のような“交番論理系”が提唱される。

4．1　交番論理系

交番論理系は，1つの論理変数（真理値）を2つの交番的（相補的）情報の時間的系列からなる2-tupleで表現し，かつ，通常の論理系と同様，所与の論理動作を行うものである。

本稿では，真理値"0"　$\longleftrightarrow$　交番情報（0，1）

　　　　真理値"1"　$\longleftrightarrow$　交番情報（1，0）

　　　　変数　X　$\longleftrightarrow$　交番情報（X，$\bar{X}$）

なる対応付けを考える。

一般に論理関数 $f(X)$ を実行する交番論理系は，入力変数Xに対応する交番入力（変数），（X，$\bar{X}$）を印加するとき，$f(X)$ に対応する交番出力 $\mathcal{F}_f \triangleq (\mathcal{F}_f^A(X), \mathcal{F}_f^B(\bar{X}))$；

(i)　$\mathcal{F}_f^A(X) = \overline{\mathcal{F}_f^B(\bar{X})}$

(ii)　$f(X) = \alpha \Rightarrow (\mathcal{F}_f^A(X), \mathcal{F}_f^B(\bar{X})) = (\alpha, \bar{\alpha})$

となるものと考えられるが，

$$\mathcal{F}_f^A(X) = f(X), \quad \mathcal{F}_f^B(\bar{X}) = f^D(\bar{X})$$

とするのが最も自然であろう。

残りの非交番的情報からなる2-tupleは，

$\Phi \triangleq \{$"0"（0，1），"1"（1，0）$\}$

とdisjointな"Φ_α"形故障（誤り）を表示する。

$\Phi_\alpha \triangleq \{$（0，0），（1，1）$\}$

4．2　交番論理系の構成

A. 基本交番論理系による構成

（i）交番論理和回路　$\vee_{\textcircled{A}} = (\vee, \wedge)$

論理関数　：$f_{\vee}(X_1, X_2) = X_1 + X_2$

交番出力関数：$\mathcal{F}^{A}_{f_{\vee}}(X_1, X_2) = X_1 + X_2$

$$\mathcal{F}^{B}_{f_{\vee}}(\overline{X}_1, \overline{X}_2) = \overline{X}_1 \cdot \overline{X}_2$$

（ii）交番論理積回路　$\wedge_{\textcircled{A}} = (\wedge, \vee)$

（iii）交番論理否定回路 $N_{\textcircled{A}} = (N, N)$ or 信号交換

従って，基本交番論理回路：$\vee_{\textcircled{A}}$〔$\wedge_{\textcircled{A}}$〕は $\vee$ と $\wedge$〔$\wedge$ と $\vee$〕の機能を交番的に遂行するものといえるが，可変閾値閾値論理素子の閾値を適当に選定することにより実現される。

自己双対論理関数である論理否定の場合には，通常の否定回路に交番入力（X, $\overline{X}$）を印加するとき交番論理系が実現される。また，交番論理否定は２つの交番的（相補的）信号を時間的に入れ換えるものと考えられるから，その手段が許される物理系を用いるならばさらに簡単な構成となる。

このとき，"与えられた論理関数 $f(X)$ の交番論理系は $f(X)$ を実行する通常の論理和，論理積，論理否定回路からなる論理系において各論理回路を交番論理回路で置換えることにより構成される。"

基本交番論理回路の故障検出：

基本交番論理回路には次の2種類の故障；

（i）真理値固定故障……交番論理回路の出力が入力とは無関係に（0，0）または（1，1）に固定する。

（ii）機能固定故障……交番論理回路，V$_{⊗}$，Λ$_{⊗}$において，その機能が論理和，論理積の一方に固定する

が予想される。

一般に，交番論理系の故障検出を出力端における誤り信号（0，0）または（1，1）の検出（“Φ_α”形故障検査）によってのみ行うものとすれば，

“基本交番論理回路；V$_{⊗}$，Λ$_{⊗}$，N$_{⊗}$で構成される任意の交番論理系において，一つの基本論理回路が故障するとき，系の出力は論理的に正しい交番出力または“Φ_α”形故障検査可能な出力である。”

B．自己双対論理関数交番論理系

所与の論理関数 $f(X)$ が自己双対であるとき，その $f(X)$ を実現する通常の論理系に交番入力（X，$\overline{X}$）を印加することにより所望の交番出力 F_f が得られる。

ところで，n 変数自己双対論理関数族は完全系をなし得ないから，“任意の n 変数論理関数は高々1個の冗長入力により自己双対化可能”であることが利用される。（この構成では

単なる2重系構成によるより少ない基本論理回路で実現される論理関数の例が得られる。）

"所与の自己双対論理関数 $f(X)$ を実行する交番論理系 : $T_f(X, \bar{X}) = (T_f^A(X), T_f^B(\bar{X})) = (f(X), f(\bar{X}))$ において故障の生起する部位（gate）の部分論理関数を $g(X)$ とする。このとき、$f(X)$ が $g(X)$ について正または負であるならば、$g(X)$ の "0" または "1" への固定と等価な故障による出力誤りは (α, α) に限られる。"（$\alpha = 0$ or 1）.

4．3．交番論理系の Fail-Safe 性

空間的2重論理系である Double Rail 論理系で考察したものとアナロジカルに

$$\Psi = \{ \text{"0"}(0, 1), \ \text{"1"}(1, 0) \}$$

$$\Phi_\alpha = \{ (\alpha, \alpha) \} \qquad \alpha = 0 \ {}^{\text{and}}/_{\text{or}} \ 1$$

とすることにより "Φ_α" 形 Fail-Safe 交番論理系を定義するのが妥当と思われる。即ち、"ある交番論理系に生起する全ての障害に対して可能な誤り出力が $\{(\alpha, \alpha)\}$ に限られるとき、系は "Φ_α" 形 Fail-Safe 交番論理系である" という。これは前節の "Φ_α" 形故障検出可能性と同値であるから、基本交番論理回路に2値的（双方向、対称）故障が予想されるとき、その交番論理系の出力成分関数 T_f^A と T_f^B のいずれか

がerror-freeである限りにおいて "Ⅱα" 形 Fail-Safe性が保存されるのである。

このような "Ⅱα" 形 Fail-Safe性をより確実なものとするために、一方向（非対称）誤り基本論理回路の存在を仮定する場合についても、前述の結果から容易に推察されよう。

以上、筆者らが行ってきたFail-Safe論理系構成に関する研究をまとめ、多値論理の応用例としても興味深い性質が含まれていることについて述べてきた。

最後に日頃から御指導いただく本学の平山博教授に深く感謝する。Fail-Safe論理系に関して終始適切な御助言をいただく国際電々研究所渡辺昭治博士に深謝する。また、交番論理系については、その多くが国際電々研究所山本幸雄氏によっていることを付記し、同氏に感謝の意を表します。

文献

〔1〕 渡辺，高橋："フェイルセイフ形論理系の一構成法" 信学全大 72 (1965-11)

〔2〕 渡辺，浦野："パラメトロンによる準Fail-Safe論理系" 信学電算研資 (1966-12)

〔3〕 渡辺，浦野："Fail-Safe論理系" 信学誌 50 2 p.p. 290-291 (1967-02)

〔4〕 浦野，平山，渡辺："φ型Fail Safe論理系" 信学オートマトン研資 A 67-41 (1967-11)

〔5〕 平山，渡辺，浦野："Fail-Safe論理系の構成理論" 信学論誌 52-C 1 p.p. 33-40 (1969-01)

〔6〕 浦野，平山："Φ型Fail-Safe論理系の構成" 信学電算研資 EC 68-34 (1969-01)

〔7〕 向殿，土屋，駒宮："C形フェイルセイフ論理回路の数学的構造について"(1)，(2) 信学電算研 EC 67-30 (1968-02)，EC 68-6 (1968-05)

〔8〕 橋本，都倉，嵩："非対称誤り素子によるフェイルセイフ論理回路と2重化論理" 信学誌 50 4 p.p. 680-687 (1967-04)

〔9〕 Mine，Koga："Basic Properties and a Construction Method for Fail-Safe Logical Systems"

I.E.E.E. Trans. on E.C EC-16 3 pp. 282-289 (1967-06)

〔10〕 三根, 高岡: "非対称故障論理回路を用いた二重系の一構成法" 信学オートマトン研資 (1967-09)

〔11〕 中嶋: "フェイルセイフ論理回路とその無接点継電器系への応用" 制御工学 13 2 (1969-02)

〔12〕 山本, 渡辺, 浦野: "交番論理系とその故障検出への応用": 信学電算研資 EC 69-15 (1967-07)